DEPARTMENT OF STATE

STATEMENT

OF

BRENDA S. SPRAGUE

DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

HEARING

ON

GOVERNMENT ISSUED IDENTIFICATION CARDS

WEDNESDAY, June 19, 2013

Thank you for the opportunity to testify today about the Department of State's role in the U.S. ePassport and Passport Card programs.

I think we all agree: The integrity of the U.S. passport is essential to our national security and the protection of our traveling citizens. By U.S. Passport, I am referring to both the Passport Book and Passport Card. At the Department of State, we believe that issuing secure travel documents to qualified citizens is a cornerstone of our national mandate. In pursuit of this, we've spent years creating a physical passport with security features, a photo biometric, and enhanced electronics that render a U.S. ePassport virtually impossible to counterfeit.

We are proud of this achievement, but we are not resting on our laurels. We are well into the planning and development process for the next generation passport. We have gathered an elite team of experts on document security and design and border control systems from across the Bureaus of Consular Affairs and Diplomatic Security, the Department of Homeland Security's (DHS) Customs and Border Protection (CBP) and Immigration and Customs Enforcement, the Bureau of Engraving and Printing, and the Government Printing Office's (GPO) Security and Intelligent Documents office to serve on the Next Generation Passport Working Group.

The Group is charged with evaluating passport design concepts and new technologies and developing recommendations based on their relative impact and advantages. The group is looking at the possible use of laser engraving on a plastic bio-page which would allow the Department of State to leverage the enhanced security found in the Passport Card for the passport book. Also, we are looking at laser perforating the pages of the passport to help combat page substitution, a feature commonly found in the passports of other countries.

The Department plans to deploy the next generation passport in 2015. This timeline includes extensive testing of the durability of the new passport and its ability to withstand alteration and counterfeiting attempts. These tests are conducted with industry experts in the areas of product durability, operations, and adversarial analysis within the government and in the private sector.

The Department of State prefers for the components of the passport book, particularly the chip, to be "Made in America" as much as possible. GPO, which manages the contractual relationship with vendors that supply the materials for the passport book, has successfully engaged suppliers and now almost all components and raw materials for the passport book are made in the United States.

Having a high-quality physical document is not enough. It is only in conjunction with our highly-trained passport adjudicators and fraud prevention managers that access to the document remains secure.

The dedication and expertise of these employees not only helps protect our borders, it also helps drive our economic engine – ensuring U.S. citizens can travel for work, for pleasure, and to visit family and friends abroad.

Passport adjudicators spend hours annually in mandated training to make certain their skills are up to this demanding task. We've also built anti-fraud tools into the adjudication process to assist them in this endeavor.

Passports are issued based on review of citizenship and identity documents issued by federal, state, and local jurisdictions. Our ability to verify the accuracy and authenticity of those documents is greatly enhanced by real-time information sharing and cooperation with the issuing agencies.

In the last six months, we have incorporated the FBI's National Criminal Information Center NCIC Supervised Release files and a real time Social Security

check into our front-end verification process. Additionally, we use the National Law Enforcement Telecommunications System network to verify driver's licenses. We are working with state vital records bureaus to encourage participation in a national centralized database of birth and death records provided by The National Association for Public Health Statistics and Information Systems. We also use the services of several commercial data providers which allow our employees to verify an applicant's social footprint and detect fraudulent addresses, phone numbers, and other discrepancies in an applicant's data.

We believe data-sharing programs like these are essential tools for verifying the identity and entitlement of passport applicants, and we continue to pursue opportunities to expand these efforts further among federal, state, and local agencies.

Since August 2006, the ePassport has been in the vanguard of the effort to improve border security. It is fully compliant with the recommended specifications for machine-readable travel documents of the International Civil Aviation Organization (ICAO). It has printed biographical data protected with a secure laminate and many other security features to protect the integrity of the document and deter counterfeiting, including micro-printing, color-shifting

optically variable security ink, and random florescent fibers. The passport also contains an integrated circuit or chip. The personal data stored on the chip is identical to the data that is printed visually on the data page along with a digital photo image of the passport bearer.

The Department's Travel Document Issuance System (TDIS) resides on a secure State intranet. It uses data from the individual's application to create a unique, one time signature and sends that back to TDIS. That unique signature is then written to the chip, completing what we call the Public Key Infrastructure (PKI) process. The chip is then locked so that the chip can't be written to again and to prevent the data on the chip from ever being changed.

To prevent skimming and eavesdropping of data, Basic Access Control (BAC) is employed. BAC is similar to a PIN used in ATM or credit card transactions. In the case of the electronic passport, characters from the printed machine-readable zone of the passport must be read first in order to unlock the chip for reading. Thus, when an electronic passport is presented to an inspector, the inspector must scan the printed lines of data (MRZ or Machine Readable Zone) in order to be able to read the highly protected data on the chip. To further protect against skimming, the U.S. passport also includes a shielding material in the

passport cover that complicates attempts at skimming as long as the passport is closed.

Finally, in order to mitigate the ability to track individuals, the chips used in U.S. electronic passports have randomized Unique Identifiers – or UIDs. Randomized UIDs allow the U.S. passport to change its chip identifier each time it is powered up, thus preventing tracking via that number. The Department believes that the use of PKI, BAC, shielding material, and randomized UIDs mitigates the risks associated with skimming or altering data from the chip. It is highly unlikely that U.S. ePassports could be altered in any way while they are being held by a foreign inspection authority or hotel. The U.S. ePassport protects the privacy of all U.S. ePassport bearers from nefarious acts.

Biometrics provide for an added level of security to ensure that these documents are not fraudulently altered or used. Using Facial Recognition (FR), all photos submitted by passport applicants worldwide are screened against the State Department's extensive database of facial images to confirm identity as well as to detect fraudulent applications. To improve the effectiveness of our FR system, we have worked to improve the quality of the passport photo by updating our software

and implementing a printer calibration standard which allows for the printing of clearer images. We have also designed a brochure showing acceptable and non-acceptable photos which is being distributed to our more than 8,000 passport application acceptance facilities across the country.

In July 2008, the Department of State began issuing passport cards enhanced with Radio Frequency Identification (RFID) technology to allow for U.S. citizens to reenter the country via land or sea from Canada, Mexico, Bermuda, and the Caribbean as part of the Western Hemisphere Travel Initiative. The Department of State designed the new Passport Card to be as tamper and counterfeit-resistant as possible. The card has forensic security features to guard against tampering and counterfeiting and to give -CBP officers "see and feel" cues to verify the card.

We also work with CBP to evaluate the use of the RFID technology at the borders to ensure the Passport Card meets their operational needs. In previous versions of the passport card, we encountered an unacceptable read-rate. The Department instituted additional RFID testing prior to use at our personalization centers to ensure we were providing the public with the best possible product. With the release of the updated Version 3 Passport Card in summer 2012, which included improved RFID technology, and CBP's improved reader software, we

have virtually eliminated what State and CBP both considered a challenging problem.

The most obvious security feature of the passport card is the use of laser engraving which is extremely difficult to forge or counterfeit, in place of standard photo dye sublimation images used in standard identity cards. The Department is also using an optical variable device (OVD), similar to a hologram, embedded inside the card. The embedded OVD overlaps the laser-etched photograph below the card surface. Any attempt to alter the OVD or the bearer's image will destroy the integrity of the card.

To facilitate the frequent travel of U.S. citizens living in border communities and to meet DHS's operational needs at land borders, the passport card incorporates vicinity-read RFID technology. With this technology, Customs and Border Protection inspectors at U.S. land and sea ports of entry are able to verify the traveler's identity before the traveler reaches the inspection station. To protect the privacy of citizens, a protective sleeve is provided with each passport card to guard against unauthorized reading or tracking of the card when it is not in use.

We have made a few notable upgrades to the security of the passport card since its introduction in 2008. In April 2010, we introduced a secondary "Ghost" image of the bearer formed by repeated lines of text. This text, generated by a security algorithm, varies according to the bearer's personal data. In December 2012, we introduced a new composite card made almost entirely of polycarbonate. The manufacturing process of this new card fuses each layer so that it makes layer separation extremely difficult.

Before releasing a new version of the passport card, we require many different testing protocols. As the card is valid for 10 years, we conduct rigorous durability tests at different stages of card manufacturing. The Department works with CBP to conduct operational testing to evaluate how the RFID chip responds to their equipment at the borders. We also work with the DHS' Homeland Security Investigations Forensic Laboratory to leverage their experiences with similar documents issued by foreign nations to evaluate the security features, construction, and personalization of the card for their opinion from a counterfeit deterrence perspective.

This multi-step approach to testing all of our documents has proven to be effective; to have the world's most secure travel documents requires that we

continually assess the security features and design of the passport and passport card for potential vulnerabilities and risks and incorporate new measures as technology advances.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.